UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/849,318	05/19/2004	Paul Gassoway	063170.7177	5789

5073 7590 01/27/2011
BAKER BOTTS L.L.P.
2001 ROSS AVENUE
SUITE 600
DALLAS, TX 75201-2980

EXAMINER	
LOUIE, OSCAR A	

ART UNIT	PAPER NUMBER
2436	

NOTIFICATION DATE	DELIVERY MODE
01/27/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ptomail1@bakerbotts.com
glenda.orrantia@bakerbotts.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/849,318
Filing Date: May 19, 2004
Appellant(s): GASSOWAY, PAUL

Paul Gassoway
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 11/15/2010 appealing from the Office action mailed 05/26/2010.

(1) Real Party in Interest

The examiner has no comment on the statement, or lack of statement, identifying by name the real party in interest in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The following is a list of claims that are rejected and pending in the application:

1-24

(4) Status of Amendments After Final

The examiner has no comment on the appellant's statement of the status of amendments after final rejection contained in the brief.

(5) Summary of Claimed Subject Matter

The examiner has no comment on the summary of claimed subject matter contained in the brief.

(6) Grounds of Rejection to be Reviewed on Appeal

The examiner has no comment on the appellant's statement of the grounds of rejection to be reviewed on appeal. Every ground of rejection set forth in the Office action from which the appeal is taken (as modified by any advisory actions) is being maintained by the examiner except for the grounds of rejection (if any) listed under the subheading "WITHDRAWN REJECTIONS." New grounds of rejection (if any) are provided under the subheading "NEW GROUNDS OF REJECTION."

(6) Grounds of Rejection to be Reviewed on Appeal

The examiner has no comment on the appellant's statement of the grounds of rejection to be reviewed on appeal. Every ground of rejection set forth in the Office action from which the appeal is taken (as modified by any advisory actions) is being maintained by the examiner except for the grounds of rejection (if any) listed under the subheading "WITHDRAWN REJECTIONS." New grounds of rejection (if any) are provided under the subheading "NEW GROUNDS OF REJECTION."

(7) Claims Appendix

The examiner has no comment on the copy of the appealed claims contained in the Appendix to the appellant's brief.

(8) Evidence Relied Upon

2005/0037733	Coleman et al.	02-2005
6,279,113	Vaidya	08-2001
7,032,114	Moran	04-2006
2004/0172557	Nakae et al.	09-2004

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-4, 7-10, 13-16, & 19-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vaidya (US-6279113-B1) in view of Coleman et al. (US-20050037733-A1).

Claims 1, 7, 13, & 19:

Vaidya discloses a computer-implemented method for maintaining security of a computer system, the computer comprising a memory and a central processing unit, a system for maintaining computer security, a computer recording medium including computer executable code for maintaining security of a computer system, and a system for maintaining computer security comprising,

- "providing access to a database of signatures" (i.e. "the data repository 12 includes a database handler 26 which polls the data collectors 10 for intrusion detection data and stores the data for future reference") [column 5 lines 47-50];
- "receiving data" (i.e. "The remote network 24 is connected to the LAN 11 and is equipped with a data collector 10 which monitors work stations located on the remote network 24 and transmits network security data specific to the remote network back to the data repository 12. Both the remote network 24 and the LAN 11 are connected to the global communications network referred to as the Internet") [column 5 lines 39-46];
- "comparing the received data with the database of signatures" (i.e. "The attack signature profiles are adapted for detecting network data patterns associated with network intrusions which include unauthorized attempts to access network objects, unauthorized manipulation of network data, including data transport, alteration or deletion, and attempted delivery of malicious data packets capable of causing a malfunction in a network object") [column 5 lines 33-39];

but, Vaidya does not explicitly disclose,

- "determining an initial system certainty value for the computer system," although Coleman et al. do suggest a mistrust level for each wireless network device, as recited below;

- "each signature including a signature certainty value," although Coleman et al. do suggest a confidence level with respect to a detected anomaly, as recited below;
- "increasing the system certainty value if the received data does not match a signature in the database" and "decreasing the system certainty value if the received data matches a signature in the database," although Coleman et al. do suggest incrementing/decrementing the mistrust level accordingly, where although the incrementing and decrementing are done on inverse conditions as compared to the applicant's claims (i.e. the prior art decrements whereas the applicant increments under the same condition); Coleman et al. also do suggest that the calculation methodology can be modified; additionally, it is reasonable to expect one of ordinary skill in the art to view the incrementing/decrementing as a design decision so long as the incrementing is opposite of the decrementing in terms of the matched conditions; that is, incrementing the mistrust level can be for a match so long as decrementing the mistrust level is for a no match and vice versa, as recited below;
- "filtering the data based on the system certainty value and the signature certainty value of a signature matching the received data," although Coleman et al. do suggest utilizing both the confidence value and initial mistrust level to calculate a new mistrust level to determine the intrusion prevention measures to enact, as recited below;

however, Coleman et al. do suggest , as recited below;

- "...The RIAFE 86 maintains a running mistrust level for each wireless network device 36, 38 and each WiAP 16, 16' in the WiNet 18 based on WiNet 18 traffic/event data 100 received at CDE 76. Based on the confidence metric and the type of anomaly detected (e.g., received as decision data from the CDE 76), different attacks are assigned different weights…For example, a detected RF anomaly is assigned weight .alpha. whereas a digital signature mismatch is assigned a different weight .beta.. The mistrust level of network devices 34, 36 and WiAPs 16, 16' is initialized to zero, then incremented and/or decremented by the RIAFE 86…" [page 6 para 102-103];

- "…The confidence level corresponding to the detected anomaly for that wireless network device…" [page 8 para 118];
- "…The RIAFE 86 maintains a running mistrust level for each wireless network device 36, 38 and each WiAP 16, 16' in the WiNet 18 based on WiNet 18 traffic/event data 100 received at CDE 76. Based on the confidence metric and the type of anomaly detected (e.g., received as decision data from the CDE 76), different attacks are assigned different weights…For example, a detected RF anomaly is assigned weight .alpha. whereas a digital signature mismatch is assigned a different weight .beta.. The mistrust level of network devices 34, 36 and WiAPs 16, 16' is initialized to zero, then incremented and/or decremented by the RIAFE 86…The mistrust level decrement value is calculated within the normal range of mistrust levels (e.g., M<4) using CDE 76 inputs is illustrated with the pseudo code in Table 4. However, the invention is not limited to this calculation and other calculations can also be used to practice the invention…" [page 6 para 102 & page 8 para 124];
- "…Also, the confidence metric is quantitative. In one embodiment of the invention, the confidence level is a real number between zero and one, and is used by the RIAFE 86 as a multiplier. However, the present invention is not limited to such a confidence level and

> other confidence levels can also be used. The confidence level corresponding to the detected anomaly for that wireless network device is multiplied by the weighting factor that is assigned to the corresponding detected anomaly, and the result is added to the existing mistrust level for the given wireless network device 36, 38 to arrive at the new mistrust level. A decrement value is also included. The mistrust level is adjusted according to Equation 9. M.sub.new=M+.alpha..beta.-M.sub.dec.sub..sub.--.sub.val, (9) where M.sub.new is a new mistrust level, M is an old mistrust level, a is a confidence level in a detected anomaly, .beta. is a weight assigned to the type of anomaly and, M.sub.dec.sub..sub.--.sub.val is a mistrust level decrement value…Pro-active intrusion prevention is achieved by dynamic switching or cycling of these protection suites according to the running mistrust levels. If a mistrust level of three is reached, more drastic intrusion prevention measures are taken, including switching of the RF band, for example, for 802.11b from 2.4 GHz to 5 GHz. This sends an alarm notification 102 to the network administrator 92…" [page 8 para 118-119 & page 9 para 130];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "determining an initial system certainty value for the computer system" and "each signature including a signature certainty value" and "increasing the system certainty value if the received data does not match a signature in the database" and "decreasing the system certainty value if the received data matches a signature in the database" and "filtering the data based on the system certainty value and the signature certainty value of a signature matching the received data," in the invention as disclosed by Vaidya for the purposes of adjusting the level of trust for a particular device based on the matches of anomalies/signatures (i.e. does the received data match a known intrusion).

Claims 2, 8, 14, & 20:

Vaidya and Coleman et al. disclose a computer-implemented method for maintaining security of a computer system, the computer comprising a memory and a central processing unit, a system for maintaining computer security, a computer recording medium including computer executable code for maintaining security of a computer system, and a system for maintaining computer security, as in Claims 1, 7, 13, & 19 above, their combination further disclosing,

- "the data that does not match a signature in the database is forwarded to its destination" (i.e. "indicating which network objects are not permitted to access other network objects") [column 6 lines 34-35].

Claims 3, 9, 15, & 21:

Vaidya and Coleman et al. disclose a computer-implemented method for maintaining security of a computer system, the computer comprising a memory and a central processing unit, a system for maintaining computer security, a computer recording medium including computer executable code for maintaining security of a computer system, and a system for maintaining computer security, as in Claims 1, 7, 13, & 19 above, but Vaidya does not explicitly disclose,

- "the increased or decreased certainty value becomes the initial system value," although Coleman et al. do suggest incrementing/decrementing the mistrust level accordingly, as recited below;

however, Coleman et al. do disclose,

- "...The RIAFE 86 maintains a running mistrust level for each wireless network device 36, 38 and each WiAP 16, 16' in the WiNet 18 based on WiNet 18 traffic/event data 100 received at CDE 76. Based on the confidence metric and the type of anomaly detected (e.g., received as decision data from the CDE 76), different attacks are assigned different weights...For example, a detected RF anomaly is assigned weight .alpha. whereas a digital signature mismatch is assigned a different weight .beta.. The mistrust level of network devices 34, 36 and WiAPs 16, 16' is initialized to zero, then incremented and/or decremented by the RIAFE 86...The mistrust level decrement value is calculated within the normal range of mistrust levels (e.g., M<4) using CDE 76 inputs is illustrated with the pseudo code in Table 4. However, the invention is not limited to this calculation and other calculations can also be used to practice the invention..." [page 6 para 102 & page 8 para 124];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the increased or decreased certainty value becomes the initial system value," in the invention as disclosed by Vaidya for the purposes of adjusting the level of trust for a particular device based on the matches of anomalies/signatures (i.e. does the received data match a known intrusion).

Claims 4, 10, 16, & 22:

Vaidya and Coleman et al. disclose a computer-implemented method for maintaining security of a computer system, the computer comprising a memory and a central processing unit, a system for maintaining computer security, a computer recording medium including computer executable code for maintaining security of a computer system, and a system for maintaining computer security, as in Claims 1, 7, 13, & 19 above, their combination further disclosing,

- "the data comprises a packet of data" (i.e. "data packets") [column 5 line 38].

3. Claims 5, 11, 17, & 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vaidya (US-6279113-B1) in view of Coleman et al. (US-20050037733-A1) in view of Nakae et al. (US-20040172557-A1).

Claims 5, 11, 17, & 23:

Vaidya and Coleman et al. disclose a computer-implemented method for maintaining security of a computer system, the computer comprising a memory and a central processing unit, a system for maintaining computer security, a computer recording medium including computer executable code for maintaining security of a computer system, and a system for maintaining computer security, as in Claims 1, 7, 13, & 19 above, but their combination do not explicitly disclose,

- "the filtering further comprises forwarding the data if the signature certainty value is less than the system certainty value," although Nakae et al. do suggest the confidence level exceeding the threshold value, as recited below;

- "the filtering further comprises discarding the data if the signature certainty value is greater than the system certainty value," although Nakae et al. do suggest blocking access when the confidence does not exceed the threshold, as recited below;

however, Nakae et al. do disclose,

- "After the confidence level c has exceeded the threshold value T, the IP packets of the access from the ordinary host 302 are guided to the server 401 on the internal network 4" [page 11 para 193 lines 16-19];
- "This causes input IP packets to be continuously guided to the decoy unit. Thereafter, when detecting an attack corresponding to "intrusion" or "destruction", the permanent access blocking is made active" [page 14 para 249 lines 7-11];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the filtering further comprises forwarding the data if the signature certainty value is less than the system certainty value" and "the filtering further comprises discarding the data if the signature certainty value is greater than the system certainty value," in the invention as disclosed by Vaidya and Coleman et al. for the purposes of providing a determination as to whether a requester is permitted or denied access to the network according to a level of trust.

4. Claims 6, 12, 18, & 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vaidya (US-6279113-B1) in view of Coleman et al. (US-20050037733-A1) in view of Nakae et al. (US-20040172557-A1) in view of Moran (US-7032114-B1).

Claims 6, 12, 18, & 24:

Vaidya, Coleman et al., and Nakae et al. disclose a computer-implemented method for maintaining security of a computer system, the computer comprising a memory and a central processing unit, a system for maintaining computer security, a computer recording medium including computer executable code for maintaining security of a computer system, and a system for maintaining computer security, as in Claims 1, 7, 13, & 19 above, but their combination do not explicitly disclose,

- "the step of forwarding further comprises generating a message log to indicate that data matching a signature was forwarded," although Moran does suggest an event record, as recited below;

however, Moran does disclose,

- "an intrusion detection system comprises a mechanism for checking timestamps, configured to identify backward and forward time steps in a log file, filter out expected time steps, correlate them with other events, and assign a suspicion value to a record associated with an event" [column 4 lines 28-33];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the step of forwarding further comprises generating a message log to indicate that data matching a signature was forwarded," in the invention as disclosed by Vaidya, Coleman et al., and Nakae et al. for the purposes of recording timed information for future further analysis.

(10) Response to Argument

a. Response to Appellant's arguments sections 1-4: Claims 1-4, 7-10, 13-16, and 19-22 are obvious over Vaidya in view of Coleman; Claims 5, 11, 17, and 23 are obvious over Vaidya in view of Coleman in view of Nakae; Claims 6, 12, 18, and 24 are obvious over Vaidya in view of Coleman in view of Nakae in view of Moran.

- ***Appellant's argument section "I. Legal Standard for Obviousness" (see pages 15*-16 of *appellant's brief):***
  - The combination of the prior art references teach or suggest all of the claim limitations as shown above and are elaborated below in response to the appellant's detailed arguments.

- ***Appellant's argument section*** **"<u>II. Claims 1-4, 7-10, 13-16, and 19-22 are Allowable over Vaidya in view of Coleman</u>"** ***subsection*** **"<u>A. Claims 1-2, 4, 7-8, 10, 13-14, 16, 19-20, and 22</u>" (see pages 17-19** ***of appellant's brief):***
    - The appellant's argument "…Thus, the mistrust levels disclosed in <u>Coleman</u> correspond to individual levels associated with wireless network device located within a computer system. There is no disclosure, teaching, or suggestion of a single initial system certainty value for the computer system. Accordingly, <u>Coleman</u> and the proposed <u>Vaidya-Coleman</u> combination, as relied upon by the Final Office Action, does not disclose, teach, or suggest "determining an initial system certainty value for the computer system," as recited in Claim 1…" has been carefully considered but is non-persuasive because <u>Coleman et al.</u> do teach a "mistrust level" which is assigned to each wireless device as a value "initialized to zero" [<u>Coleman et al.</u> page 6 para 103] and then adjusted by increasing/decreasing the value based on the detection of an anomaly [<u>Coleman et al.</u> page 6 paras 100, 102, 103];
        - It is noted that the appellant's claim language does not clearly claim that the entire computer system itself performs the determination of the initial system certainty value for the computer system itself based on the detection of intrusions in the incoming data packets; therefore, given the broadest most reasonable interpretation of the appellant's claims, the limitations which pertain to "determining an initial system certainty value for the computer system" can be viewed as either an external system

which assigns a “certainty value” to other devices connected to the system or that the system comprises the intrusion detection/prevention system coupled to one or more devices which are assigned a “certainty value” by the intrusion detection/prevention portion of the system;

- The appellant’s arguments “...Coleman fails to disclose, teach, or suggest the "increasing the system certainty value if the received data does not match a signature in the database" and "decreasing the system certainty value if the received data matches a signature in the database," as recited in Appellant's Claim 1...” and “...While Coleman does disclose incrementing and decrementing the mistrust levels assigned to the devices, Appellant respectfully contends that these changes are not based on either matching or not matching signatures. For instance, Coleman clearly states throughout that "mistrust level decrementing is accomplished based on three parameters, described as follows: (1) a decrement timer Dl exceeds a mistrust level decrement interval from the operational protection suite; (2) mistrust level four has been reached, the wireless network device 36, 38 successfully re-authenticates, and re-login is also successful; (3) manual intervention 90 from the network administrator 92." (Coleman, paragraph 0121). Therefore, Coleman discloses a decrementing step based & on timing, manual intervention, or re-authentication...” and “...Coleman merely discloses decrementing the mistrust level if a predetermined amount of time passes and no anomalous event is detected, if the device is re-authenticated, or if the network administrator intervenes. There is no disclosure, teaching, or suggestion that matching or not matching a signature plays any role in this step…" and "…Appellant respectfully maintains that Coleman discloses "decrementing" based only on the three criteria listed above. This fails to disclose a decrementing step based on "any criteria that are deemed as an intrusion that is then matched." Therefore, even under the Office Action's proposed "broadest" interpretation, this cited portion fails to disclose, teach, or suggest "decreasing the system certainty value if the received data matches a signature in the database," as recited in Claim 1…" have been carefully considered but are non-persuasive because Coleman et al. do teach a "mistrust level" which is adjusted by increasing/decreasing the value based on detection of an anomaly, where an anomaly is typically determined based on an intrusion/attack signature that identifies each type of anomaly detected, as taught by both Vaidya, "The attack signature profiles are adapted for detecting network data patterns associated with network intrusions which include unauthorized attempts to access network objects, unauthorized manipulation of network data, including data transport, alteration or deletion, and attempted delivery of malicious data packets capable of causing a malfunction in a network object" (i.e. "anomalies") [Vaidya column 5 lines 33-39] and Coleman et al. "The CDE 76 collects wireless event data 100 and looks for normal wireless events and abnormal wireless events using a wireless event anomaly profiler 78, wireless normal event profile database 80, wireless event misuse rules 82 as is explained below…Based on the confidence metric and the type of anomaly detected (e.g., received as decision data from the CDE 76), different attacks are assigned different weights…a detected RF anomaly is assigned weight .alpha. whereas a digital signature mismatch is assigned a different weight .beta.. The mistrust level of network devices 34, 36 and WiAPs 16, 16' is initialized to zero, then incremented and/or decremented by the RIAFE 86…" (i.e. "anomalies") [Coleman et al. page 6 paras 100, 102, 103];

  - It is noted that the appellant's "decreasing" is equated to Coleman et al.'s "incrementing" since the appellant's "decrementing" is a decrease in trust of the system which is equivalent to Coleman et al.'s "incrementing" which is an increase in the severity of distrust of a particular wireless device; therefore, Coleman et al.'s "decrementing" is equivalent to the appellant's "increasing";

- ***Appellant's argument subsection* "<u>II. Claims 1-4, 7-10, 13-16, and 19-22 are Allowable over Vaidya in view of Coleman</u>" *subsection* "<u>B. Claims 3, 9, 15, and 21</u>" (see pages 20-*21 of appellant's brief):***
  - o The appellant's argument "…<u>Coleman</u> fails to disclose, teach, or suggest a "system certainty value." Rather, the mistrust levels disclosed in <u>Coleman</u> correspond to individual levels associated with each wireless network device located within a computer system. (<u>Coleman</u>, paragraph 102). Furthermore, the cited portion of <u>Coleman</u> merely discloses that the mistrust level for individual network devices is "initialized to zero, then incremented and/or decremented."

(Coleman, paragraph 0102). Specifically, Coleman discloses that "mistrust level decrementing is accomplished based on three parameters, described as follows: (1) a decrement timer Dl exceeds a mistrust level decrement interval from the operational protection suite; (2) mistrust level four has been reached, the wireless network device 36, 38 successfully re-authenticates, and re-login is also successful; (3) manual intervention 90 from the network administrator 92." (Coleman, paragraph 0121). Thus, Coleman merely discloses decrementing the mistrust level if a predetermined amount of time passes and no anomalous event is detected, if the device is re-authenticated, or if the network administrator intervenes. With regard to the actual decrementing of the mistrust level, Coleman provides an Equation 9 for calculating the new mistrust level. (Coleman, paragraph 11 8). The equation takes into account the old mistrust level, a weighted anomaly, and a mistrust level decrement value. Thus, the new mistrust level is calculated using a predetermined calculation having multiple variables. There is no disclosure that "the increased or decreased certainty value becomes the initial system value," as recited in Claim 3…" has been carefully considered but is non-persuasive because Coleman et al. do disclose initializing the mistrust level to zero and then incrementing/decrementing the mistrust level one or more times based on detected anomalies, where by definition, the current mistrust level after each increment/decrement would be the new "initial system certainty value"; that is, when the next determination is made to further increment/decrement the mistrust level, the newly adjusted mistrust level is the new "initial system certainty value," even if the mistrust level has been reset by re-initialization to zero, the current mistrust level would be the new initial system certainty value since "initial" is dependent on the perspective and point in time in which a value is considered to be "initial";

- *Appellant's argument section* **"<u>III. Claims5, 11, 17, and 23 are Allowable over the Proposed Vaidya-Coleman-Nakae Combination</u>"** *(see page 22 of appellant's brief):*
    - The Appellant's above dependent claims are obvious over the teachings by the prior art of record above.

- *Appellant's argument section* **"<u>IV. Claims 6, 12, 18, and 24 are Allowable over the Proposed Vaidya-Coleman-Nakae-Moran Combination</u>"** *(see page* 23 *of appellant's* **brief):**
    - The appellant's argument "..."generating a message log to indicate that data matching a signature was forwarded." In the Final Office Action, the Examiner admits that <u>Vaidya</u>, <u>Coleman</u>, and <u>Nakae</u> fail to disclose this limitation and relies instead on <u>Moran</u>. Appellant respectfully disagrees. The cited portion discloses "a mechanism for checking timestamps, configured to identify backward and forward time steps in a log file." (<u>Moran</u>, Column 4, lines 28-31). While this discloses identifying time stamps in a log file, <u>Moran</u> fails to disclose. teach, or suggest actually generating a log file, much less a log file that indicates that data matching a signature was forwarded. Accordingly, <u>Moran</u> and the proposed

Vaidya-Coleman-Nakae-Moran combination fails to disclose, teach, or suggest "wherein the step of forwarding further comprises generating a message log to indicate that data matching a signature was forwarded," as recited in Claim 6…" has been carefully considered but is non-persuasive because Moran suggests several methods of utilizing log files/logging for event correlation, for example:

- "…some tools allow a system administrator to be alerted whenever an entry matching any of the patterns he has specified is written to a designated log file…" [Moran column 10 lines 50-53] suggests writing events to a log file and forwarding an alert to a system administrator when an intrusion pattern is matched (i.e. "…identify backward and forward time steps in a log file, filter out expected time steps, correlate them with other events…") [Moran, Column 4, lines 28-31];
- "…Some of the programs most likely to be involved in an attack produce log entries for significant events. Some of these put related, often overlapping, information into different log files…" [Moran column 11 lines 41-44] suggests that programs involved in an attack can produce log file entries for events that are deemed as important (i.e. "…in a log file…correlate them with other events…") [Moran, Column 4, lines 28-31];

- "...when a valid username-password pair is entered, the login process writes a record to the utmp and wtmp files and updates the lastlog file..." [Moran column 20 lines 1-3] suggests writing/recording a log file entry when a valid username-password is passed/forwarded through the login process (i.e. "...identify backward and forward time steps in a log file...") [Moran, Column 4, lines 28-31];
- "...syslog is a unified logging mechanism that can be written to by any program running on the system, and it is widely used by server programs and other programs that typically run in the background. syslog messages are assigned a facility and a logging level. The system administrator uses these values to specify, via the syslog.conf file, how these messages coming from various programs should be handled: they can be discarded or directed to various log files, the host's console, specified users, other hosts, etc..." [Moran column 20 lines 27-35] suggests a specific type of logging system called "syslog" which can be configured to log any desired events (i.e. "...an intrusion detection system comprises a mechanism for checking timestamps, configured to identify backward and forward time steps in a log file, filter out expected time steps, correlate them with other events...") [Moran, Column 4, lines 28-31];

- ***Further elaboration of "filtering the data based on the system* certainty value and the *signature certainty value of a signature matching the received data" for appellants:***
    - <u>Coleman et al.'s</u> "mistrust level" is equivalent to the appellant's "system certainty value" and <u>Coleman et al.'s</u> "confidence level" ("confidence level" corresponds to the detected anomaly) is equivalent to the appellant's "signature certainty value" where the association of the "mistrust level" and "confidence level" determine the "intrusion prevention measures to take" (i.e. "filtering the data").

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Oscar A. Louie

01/12/2011

/OAL/

Conferees:

/Nasser Moazzami/

Supervisory Patent Examiner, Art Unit 2436

/Eleni A Shiferaw/

Primary Examiner, Art Unit 2436